Threat-Informed Defense

November 3, 2022

Agenda

- MITRE – What is it and how to leverage it
- Modern Day Threats and “Pain”
- MITRE – Threat-Informed Defense
- Summary & Resources

MITRE

Not-for-profit company to provide engineering and technical guidance for the federal government.

Created an advanced air-defense framework for the Air Force.
out of MIT laboratories
Est. 1958

MITRE CVE®

Invented the concept of a CVE (Common Vulnerability & Exposures)

Bridging the gap between Gov & Industry

Sponsored by CISA (DHS)
Est. 1999

MITRE ATT&CK™

A Real-World TTP Knowledgebase

Cyber adversary
Model describing Tactics, Techniques and Procedures

The foundation of Threat-Informed Defense

Est. 2013-15

MITRE ENGENUITY™
A Foundation for Public Good

ATT&CK® Evaluations

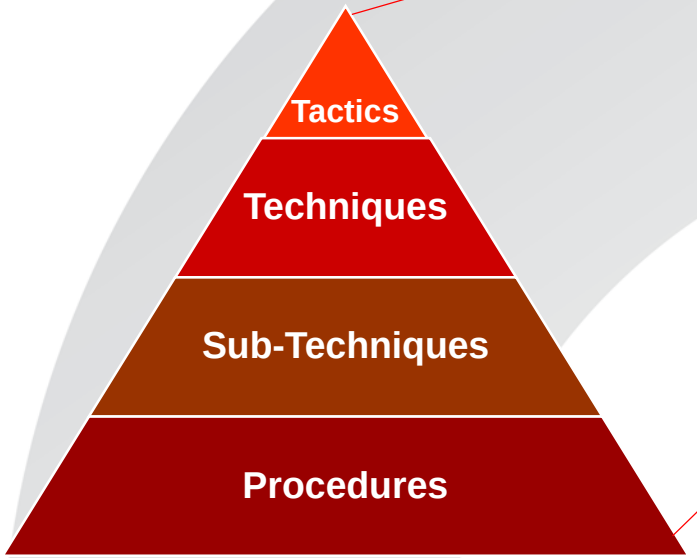
2019 – Gothic Panda
2020 – Cozy Bear
2021 - Carbanak + FIN7
2022 – Wizard Spider + Sandworm

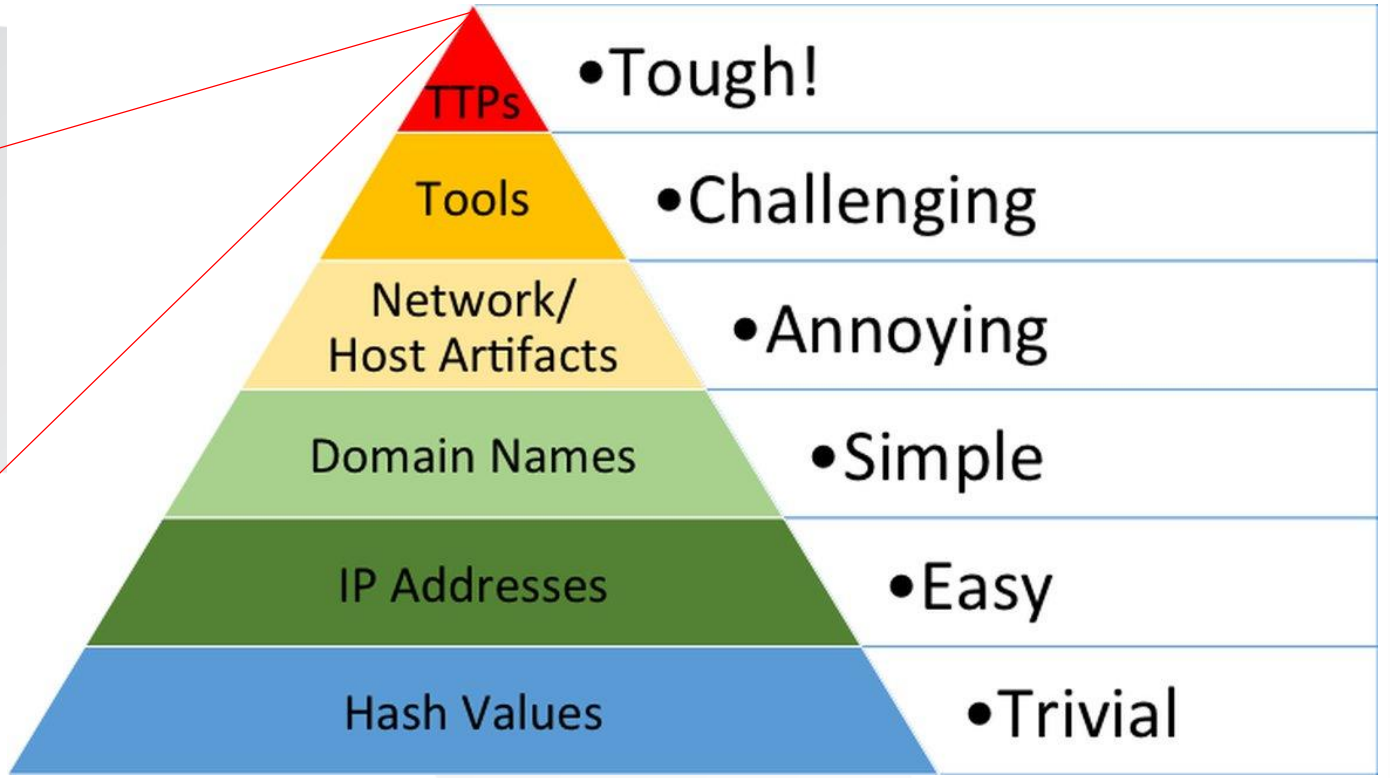
MITRE ATT&CK Defender™

Leveraging MITRE ATT&CK Framework

- Best measurement of capability
- Historical Visibility & Analytics
- Protections and detection capability
- Identify gap areas with current tooling

- Quickly understand **Why** & **How** the Attack Happened
- Faster Mean Time to Detect (MTTD)
- Improves Mean Time to Respond (MTTR)





The Pyramid of PAIN
"David J. Bianco"

"Threat-informed defense" applies a deep understanding of adversary tradecraft and technology to protect against, detect, and mitigate cyber-attacks. It's a community-based approach to a worldwide challenge." [1]

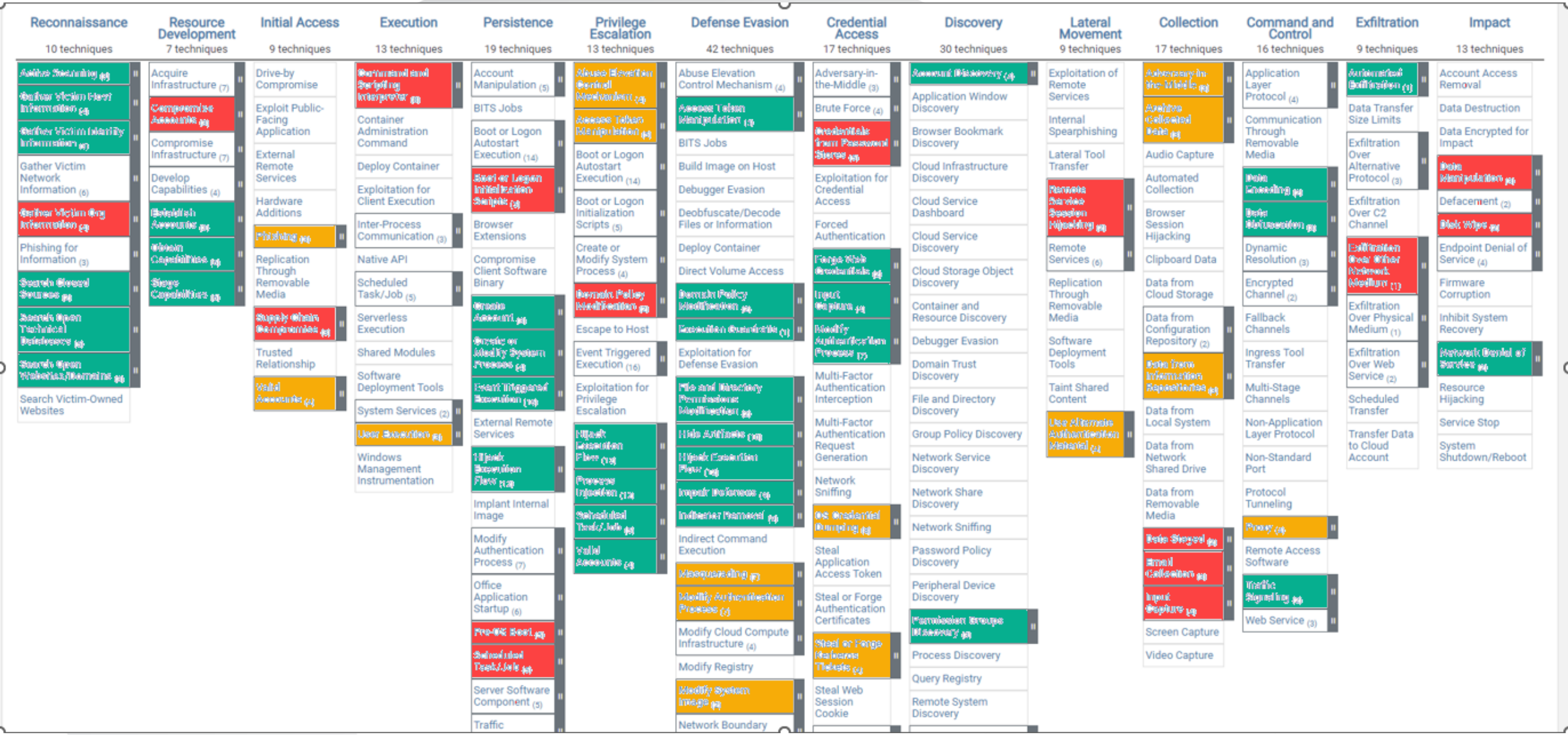
- MITRE

MITRE ATT&CK Defender™

SHI

https://www.mitre.org/news/focal-points/threat-informed-defense

MITRE ATT&CK Matrix



Summary

- Threat-Informed Defense
  - Optimize Cybersecurity programs (People, Process, and Technology)
  - Continuous validation of security controls
  - Evolve from reactive to proactive (CTI+ATT&CK)
  - Focus on threats that matter most
  - Visibility / Effectiveness

Resources

Information

- https://attack.mitre.org/
- medium.com/mitre-attack
- twitter.com/MITREattack
- linkedin.com/showcase/mitre-att&ck
- https://www.attackiq.com/threat-informed-defense/

Training

- https://attack.mitre.org/resources/training/

Mitigations

- https://attack.mitre.org/mitigations/enterprise/

Prioritize

- https://top-attack-techniques.mitre-engenuity.org/calculator

Thank You

SHI

Where you have the ability to provide funding specific to cyber defenses, we recommend making that dependent upon implementation and adherence to a Threat-Informed Defense strategy/program.

Relative to commercial entities, you may have to rely upon applicable regulatory requirements (e.g. PCI, SOX, cyber liability insurance requirements).